Table of Contents

13-2. Authentication, Authorization, and Accounting (

- Method lists are used to specify a sequence of methods to use for each componei method receives no response or an error condition, the next method in the list is
- Multiple AAA servers can be defined. If the first one listed doesn't respond or gen next server is tried.
- AAA servers can be grouped so that a collection of servers can be used for a spec
- Authentication can use a variety of methods, including RADIUS, TACACS+, Kerbe locally configured in the router.
- Authorization can use RADIUS and TACACS+ to authorize users to access availab
- Accounting can use RADIUS and TACACS+ to track and record the services and n users are using.
- Shared secret keys are configured in both the router and the RADIUS or TACACS interaction (including the user's password entry) is encrypted.

Configuration

1. Enable AAA functionality:

```
(global) aaa new-model
```

2. Identify one or more AAA servers.

a. Use a RADIUS server.

- (Optional) Set global defaults for all RADIUS servers.

  Set the shared router/server key:

```
(global) radius-server key {0 string | 7 string | stri
```

  The shared secret encryption key is set as *string* (a cleartext str the string, or if the string appears by itself, the string appears u router configuration. If **7** precedes it, the string is "hidden" and encrypted string in the configuration.

Set the request timeout interval:

```
(global) radius-server timeout seconds
```

After a request, the router waits for *seconds* (1 to 1000; the def response from a RADIUS server.

Set the number of request retries:

```
(global) radius-server retransmit retries
```

If no response is received from a RADIUS server, the router retr *retries* times (1 to 100; the default is 3).

Set the server deadtime:

```
(global) radius-server deadtime minutes
```

If a RADIUS server doesn't respond after the retransmit retries, mark it as "dead" for a period of time in *minutes* (0 to 1440; the soon as it is marked as dead, the router skips that server and se next available server.

- Specify one or more servers to use:

```
(global) radius-server host {hostname | ip-address} [a
  [acct-port port] [timeout seconds] [retransmit retri
  [alias {hostname | ip-address}] [key string]
```

The RADIUS server is identified by host name or IP address. You UDP ports for authentication (**auth-port;** the default is 1645) ar (**acct-port;** the default is 1646). You can override the defaults a of time the router waits for a RADIUS response with **timeout** (1 and set the number of retransmitted requests with **retransmit** (**alias** keyword can be used to define up to eight host names or l single RADIUS server name. The shared secret **key** can be set t string). Always set the key as the last argument so that any eml not be confused with other arguments.

- (Optional) Enable vendor-specific RADIUS attributes (VSAs):

```
(global) radius-server vsa send [accounting | authoriz
```

The router can recognize VSAs that comply with attribute 26 of t either **accounting** or **authorization.**

- (Optional) Enable vendor-proprietary RADIUS attributes:

```
(global) radius-server host {hostname | ip-address} no
```

The router can use IETF draft extensions for the most common v attributes.

b. Use a TACACS+ server.

- (Optional) Set the global shared router/server key for TACACS+

```
(global) tacacs-server key key
```

The shared secret encryption key is set as *string* (a cleartext str
spaces are accepted.

- Specify one or more servers to use:

```
(global) tacacs-server host hostname [port port] [time
  string]
```

The TACACS+ server is identified by host name. You can specify
with the **port** keyword (the default is 49). The amount of time tl
TACACS+ response is **timeout** in seconds. The shared secret **ke**
string (a cleartext string). Always set the key as the last argume
embedded spaces will not be confused with other arguments.

c. Use a Kerberos server.

- Create users and SRVTAB entries on the Key Distribution Center

Users and SRVTAB entries are administered on the Kerberos ser
Kerberos documentation for further instructions. The SRVTAB fil
associated keys will be imported into the router in a later step.

- Identify the Kerberos realm.

Define a default realm:

```
(global) kerberos local-realm realm
```

The router is located in the Kerberos *realm* (an uppercase text s
resources are registered to a server. This should be taken from t
parameter on the server.

Specify the Kerberos server for the realm:

```
(global) kerberos server realm {hostname | ip-address}
```

The server for the *realm* (an uppercase text string) is identified
IP address and also by the *port* used for the KDC (the default is
or IP address should be taken from the *admin_server* parameter
itself.

(Optional) Map a DNS domain or host name to the realm:

```
(global) kerberos realm {domain | hostname} realm
```

A *domain* (a fully qualified domain name with a leading dot) or a
leading dot) can be mapped to a specific *realm* (an uppercase te

- Import a SRVTAB file.

Create a DES encryption key:

```
(global) key config-key 1 string
```

A private DES key is created as key number **1** using *string* (up t alphanumeric characters). The key is used to generate DES key SRVTAB entries.

TFTP the SRVTAB file and create SRVTAB entries:

```
(global) kerberos srvtab remote tftp://hostname/filena
```

The SRVTAB file is identified by its URL using the server's host n followed by the filename. The file is retrieved via TFTP.

d. (RADIUS or TACACS+ only) Group a list of servers.

- Define a group name:

```
(global) aaa group server {radius | tacacs+} group-nam
```

A server group named *group-name* is created. The group can ide configured RADIUS or TACACS+ servers that can be used for a p service.

- Add a server to the group:

```
(server-group) server ip-address [auth-port port] [acc
```

The server at the IP address is a member of the group. You can ports for authentication (**auth-port;** the default is 1645) and ac **port;** the default is 1646).

- (Optional) Set a deadtime for the group:

```
(server-group) deadtime minutes
```

The group deadtime allows the router to skip over a group of se unresponsive and declared "dead" and send requests to the nex name. Deadtime is in *minutes* (0 to 1440; the default is 0).

3. Use AAA authentication.

a. Create a method list for an authentication type:

```
(global) aaa authentication {login | ppp | nasi | arap | en
  {default | list-name} method1 [method2 ...]
```

The method list named *list-name* is created. It contains a list of login auth to be tried in sequential order. The **default** keyword specifies a list of me lines and interfaces that are configured for default authentication. The list to the authentication type given by **login** (the login prompt on the router) the privileged EXEC command level), **ppp** (dialup access through PPP), **na** Asynchronous Services Interface), or **arap** (AppleTalk Remote Access Pro

The method keywords (*method1, method2,* ...) given in the list depend on authentication:

- **login— enable** (use the enable password), **krb5** (Kerberos 5), **krb** 5 for Telnet authentication), **line** (use the line password), **local** (us

usernames and passwords), **local-case** (use the router's list of cas usernames), **none** (use no authentication; every user is successfull **group radius** (use all listed RADIUS servers), **group tacacs+** (us servers), and **group** *group-name* (use only the servers listed in the *group-name*).

- **enable— enable** (use the enable password), **line** (use the line pas no authentication; every user is successfully authenticated), **group** listed RADIUS servers), **group tacacs+** (use all listed TACACS+ se *group-name* (use only the servers listed in the server group named

- **ppp— if-needed** (no authentication if the user is already logged in (Kerberos 5), **local** (use the router's list of usernames and passwor the router's list of case-sensitive usernames), **none** (use no authen is successfully authenticated), **group radius** (use all listed RADIUS **tacacs+** (use all listed TACACS+ servers), and **group** *group-name* servers listed in the server group named *group-name*).

- **nasi— enable** (use the enable password), **line** (use the line passw router's list of usernames and passwords), **local-case** (use the rou sensitive usernames), **none** (use no authentication; every user is s authenticated), **group radius** (use all listed RADIUS servers), **grou** listed TACACS+ servers), and **group** *group-name* (use only the ser server group named *group-name*).

- **arap— auth-guest** (allow a guest login if the user has EXEC acces guest logins), **line** (use the line password), **local** (use the router's and passwords), **local-case** (use the router's list of case-sensitive **radius** (use all listed RADIUS servers), **group tacacs+** (use all list servers), and **group** *group-name* (use only the servers listed in the *group-name*).

b. Apply the method list to a router line or interface.

- (PPP only) Authenticate on an interface.

  Select an interface:

  ```
  (global) interface type slot/number
  ```

  Enable PPP authentication on the interface:

  ```
  (interface) ppp authentication {protocol1 [protocol2 .
    [list-name | default] [callin] [one-time]
  ```

  PPP authentication can be used with one or more protocols (*prot* ...): **chap** (CHAP), **ms-chap** (Microsoft CHAP), or **pap** (PAP). Th keyword prevents additional authentication if TACACS or extend already authenticated a user. The method list is specified as *list-* methods that PPP sequentially tries. If a method list is not neede keyword causes PPP to use the default method. The **callin** keyw only inbound users, and **one-time** allows both username and pa presented in the username field.

- (Login, NASI, or ARAP only) Authenticate on a line.

  Select a line:

  ```
  (global) line {aux | console | tty | vty} line-number
  ```

A specific Aux, console, async, or virtual TTY line can be selecte
number. Add the *end-line-number* to select a range of line numt

Apply authentication to the line:

```
(line) {login | nasi | arap} authentication {default |
```

The authentication type is given as **login, nasi,** or **arap.** The m
list-name is used to authenticate users on the line. The **default**
used instead to use the default AAA authentication methods with
method list.

c. (Optional) Use the AAA banners and prompts.

- Create a login banner:

```
(global) aaa authentication banner dstringd
```

The customized banner *string* (up to 2996 characters) is displa
username login prompt. The *d* character is a delimiter (any char
appear in *string*) that must appear before and after the banner s

- Change the password prompt:

```
(global) aaa authentication password-prompt string
```

The default password prompt string is Password:. You can chan
text string; enclose it in double quotes if it contains spaces).

- Create a failed login banner:

```
(global) aaa authentication fail-message dstringd
```

The customized banner *string* (up to 2996 characters) is displa
fails. The *d* character is a delimiter (any character that doesn't a
that must appear before and after the banner string.

4. Use AAA authorization.

a. Create a method list for an authorization type:

```
(global) aaa authorization {auth-proxy | network | exec | c
  reverse-access | configuration | ipmobile} {default | lis
  method1 [method2 ...]
```

The method list named *list-name* is created. It contains a list of authoriza
tried in sequential order. The **default** keyword specifies a list of methods
and interfaces that are configured for default authorization. The list of me
authorization type given by **auth-proxy** (use specific policies per user), **n**
related service requests), **exec** (permission to run a router EXEC), **comm**
use all commands at privilege *level,* 0 to 15), **reverse-access** (permissio
Telnet connections), **configuration** (permission to enter router configura
ipmobile (permission to use IP mobility).

The method keywords (*method1, method2,* ...) given in the list are **group**
requests to the servers in the group named *group-name*), **group radius**
RADIUS server group), **group tacacs+** (send requests to the TACACS+ s

authenticated (permission is granted if the user is already authenticated authorization; every user is successfully authorized), and **local** (use the r usernames and passwords).

b. Apply the method list to a line or an interface.

- Authorize users on a line.

  Select a line:

  ```
  (global) line line-number [end-line-number]
  ```

  An Aux, console, async, or virtual TTY line can be selected with t Add the *end-line-number* to select a range of line numbers.

  Apply authorization to the line:

  ```
  (line) authorization {arap | commands level | exec | r
    [default | list-name]
  ```

  The authorization type is given as **arap** (AppleTalk Remote Acce **commands** *level* (permission to execute commands at privilege (permission to use a router EXEC shell), or **reverse-access** (pe reverse Telnet). The method list named *list-name* is used to autl line. The **default** keyword can be used instead to use the defaul methods without specifying a method list.

- (PPP only) Authorize users on an interface.

  Select an interface:

  ```
  (global) interface type slot/number
  ```

  Apply authorization to the interface:

  ```
  (interface) ppp authorization [default | list-name]
  ```

  The method list named *list-name* is used to authorize PPP users The **default** keyword can be used instead to use the default AA methods without specifying a method list.

5. Use AAA accounting (RADIUS or TACACS+ only).

a. Create a method list for an accounting type:

```
(global) aaa accounting {auth-proxy | system | network | ex
  connection [h323] | commands level} {default | list-name}
  stop-only | wait-start | none} [broadcast] group {radius
  group-name}
```

The method list named *list-name* is created. It contains the accounting m The **default** keyword specifies a method to be used on lines and interface for default accounting. The accounting type records information about **aut** events), **system** (system-level events), **network** (network-related servic (router EXEC sessions), **connection** (outbound connections from an acce performs H.323 gateway accounting for Voice over IP), and **commands** (privilege *level*, 0 to 15.

The method used for accounting can be **group** *group-name* (send records group named *group-name*), **group radius** (send records to the RADIUS s **group tacacs+** (send records to the TACACS+ server group).

The **broadcast** keyword causes records to be sent to multiple accounting accounting records are selected by **start-stop** ("start" when a process be process ends), **stop-only** (no "start" is sent; "stop" when the process enc ("start" when a process begins; the process doesn't actually begin until "s the server; "stop" when the process ends), or **none** (no accounting is per

b. (Optional) Record accounting for failed authentications:

```
(global) aaa accounting send stop-request authentication fa
```

The router sends "stop" records when a user authentication or a PPP nego

c. Apply the method list to a line or an interface.

- Perform accounting on a line.

  Select a line:

  ```
  (global) line line-number [end-line-number]
  ```

  An Aux, console, async, or virtual TTY line can be selected with t Add the *end-line-number* to select a range of line numbers.

  Enable accounting on the line:

  ```
  (line) accounting {arap | commands level | connection
    [default | list-name]
  ```

  The accounting type is given as **arap** (AppleTalk Remote Access **commands** *level* (EXEC commands at privilege *level*), **connecti** authentication), or **exec** (router EXEC shell). The method list na used for accounting on the line. The **default** keyword can be us the default AAA accounting method without specifying a method

- (PPP only) Perform accounting on an interface.

  Select an interface:

  ```
  (global) interface type slot/number
  ```

  Enable accounting on the interface:

  ```
  (interface) ppp accounting default
  ```

  The default method is used for PPP accounting on the interface.

Example

The router is configured for AAA using all three authentication, authorization, and accou RADIUS servers are identified as 192.168.161.45 and 192.168.150.91, both having the TACACS+ server is at 192.168.44.10. One local username is also defined. It is used as a the event that the AAA servers are inaccessible.

Authentication is set up for PPP access on async interfaces using the RADIUS servers, fo
authentication. Authentication is also used for login access to the router via Telnet, usin
server, then the RADIUS servers, and then local authentication.

Authorization is configured to use the RADIUS servers and local authentication for both
functions. Users entering the network via PPP and Telnet must be authorized. Accountin
the RADIUS servers for both network and exec resource reporting. The router sends acc
both PPP and router exec terminal sessions.

```
aaa new-model
radius-server host 192.168.161.45 key aAaUsInGrAdIuS
radius-server host 192.168.150.91 key aAaUsInGrAdIuS
tacacs-server host 192.168.44.10 key tacacs-server-1

aaa authentication login router-login group tacacs group radius local
aaa authentication ppp ppp-login group radius local
aaa authorization network default group radius local
aaa authorization exec default group radius local
aaa accounting network default start-stop group radius
aaa accounting exec default start-stop group radius

username admin password letmein

interface async 1
       encapsulation ppp
       ppp authentication pap ppp-login
       ppp authorization default
       ppp accounting default

line vty 0 4
       login authentication router-login
       authorization exec default
       accounting exec default
```

Cisco® Field Manual: Router Configuration

Table of Contents • Index

URL http://proquest.safaribooksonline.com/1587050242/ch13lev1sec2